TNO Information and Communication Technology

Nederlandse Organisatie voor
toegepast-natuurwetenschappelijk
onderzoek / Netherlands Organisation
for Applied Scientific Research

Eemsgolaan 3
P.O. Box 1416
9701 BK Groningen
The Netherlands

T +31 50 585 70 00
F +31 50 585 77 57
info-ict@tno.nl

TNO whitepaper

Beyond RFID: the NFC Security Landscape

Date	23 Oktober 2007
Reportnr	34613
Author(s)	Jaap-Henk Hoepman, Johanneke Siljee
Number of pages	15

Contents

1 Introduction

Near Field Communication (NFC) is quickly becoming the preferred technology for new mobile *close-contact* applications, such as smart posters, contactless payments, ticketing applications, and the like. With smart posters, for instance, the NFC device in the mobile phone reads an RFID tag embedded in a poster. Using the URL obtained from the tag, the internet-enabled phone quickly accesses additional information from the website set up by the poster publisher. In a contactless payment scenario, the user pays for goods at the counter by placing his mobile phone close to the NFC enabled payment terminal, thus using his mobile phone as a virtual wallet.

For applications like mobile payments for which the use of NFC technology is considered, security is of paramount importance. This whitepaper discusses the main risks associated with using NFC technology, and the possible countermeasures that can be used to mitigate those risks.

But first we briefly discuss NFC itself.

1.1 What is NFC

Near Field Communication (NFC) is a wireless connectivity technology that enables short-range communication between electronic devices. NFC is part of the set of connectivity technologies called Radio Frequency Identification (RFID) [1], although the focus of NFC is broader than identification. The NFC interface and protocol are defined by the ISO18092 standard [2], also known as NFCIP-1 and ECMA340. NFC operates in the 13.56 MHz RF band, which it shares with other RFID technologies such as ISO15963. The NFC protocol is compatible with the lower layers of the contactless smart card protocols ISO 14443, Mifare™, and Felica™. This means that NFC devices both read and may be able to emulate these types of cards. The “Near Field” in NFC refers to the short operating distance of 0-10 cm [3].

Each NFC device implements the architecture as shown in Figure 1. All devices have a radio frequency (RF) layer to be able to communicate over NFC, and can operate in different modes:

- Peer to peer mode: NFC devices communicate directly (peer to peer) with each other;
- Reader/writer mode: NFC devices read/write existing proximity cards[1];
- Card emulation mode (optional): NFC devices may be able to emulate proximity cards, and so be readable by existing proximity card readers.

The application layer holds the functionality that uses the underlying NFC capabilities for end-user applications like payment and ticketing.

[1] Proximity cards operate only in the proximity (typically <10 cm) of a reader

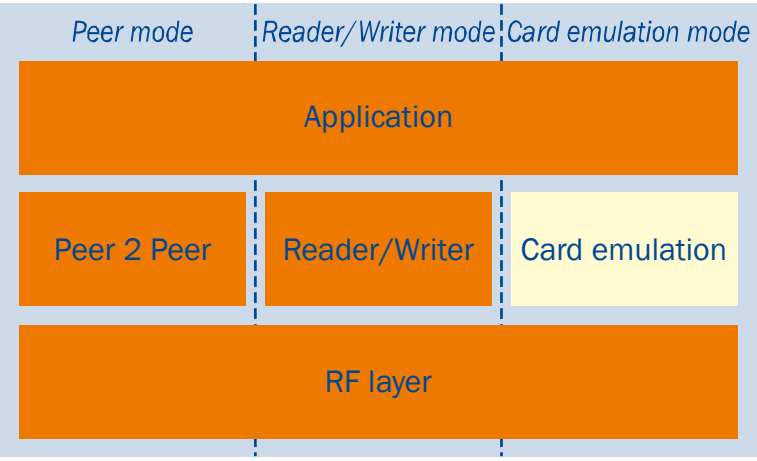

Figure 1: NFC device architecture

Compared to other communication mechanisms available, e.g. GSM, UMTS, and Bluetooth, NFC provides a small bandwidth (106-424 kbps). The major advantage is that NFC devices are *active* devices, meaning that they can initiate communication by generating an RF field that a *passive* device (smart card without battery) can use as power supply.

1.2 NFC ≠ Mifare

Many NFC applications existing today are based on Mifare. But it should be stressed that NFC is not the same as Mifare. In fact, Mifare is a proprietary specification from Philips/NXP Semiconductors that implements security features like encryption, authentication, and access control. These security features ore not part of the NFC standards.

1.3 Opportunities with NFC

It is widely believed that NFC, its little brother RFID, sensors and other similar wireless technologies, will have a tremendous impact on society. The most futuristic scenario is that of the “Internet Of Things”, that will emerge once more and more physical objects will become interconnected using these technologies. Changes brought about by the internet will be dwarfed by those prompted by the networking of everyday objects. The virtual (internet) world and the physical (real) world will merge into one gigantic network, allowing applications like “googling for your house keys”, “calling your pacemaker”, “getting warning signals from buildings before they collapse”, and many, many more.

In the near future, in fact even today, NFC is being introduced as enabling technology for contactless payments, public transport and ticketing applications.

2 Security issues of NFC

In this section we discuss the main security issues associated with NFC technology. Using NFC in a real-life application requires these issues to be addressed properly, either by implementing a countermeasure, or by making sure the specific issue does not impose a threat for the application. Possible countermeasures are discussed in the next section.

Because NFC encompasses RFID systems, threats associated with RFID are inherited by NFC. We summarise these threats first. However, NFC technology introduces its own additional security concerns as well. This is due to several factors, among which there are the size and capabilities of NFC devices, the fact that NFC devices can operate in several modes, and that more than one application may use the same single NFC interface. We discuss these new, NFC specific, threats in more detail.

2.1 RFID security threats applicable to NFC

Since NFC is strongly related to RFID, the two technologies share a number of risks. Here we summarise these risks, for more detailed information see [4, 5, 6].

- Similar to RFID tags, NFC devices like mobile phones and NFC tags may be vulnerable to ***unauthorised reading*** of information stored on the NFC device or tag, using the NFC radio interface. This threat is especially important for NFC devices and tags that store data for payment applications, like credit card information.
- Another content related threat is the ***falsification of content*** due to unauthorised writing to the data storage part of a device. Next, a *falsified unique ID* and other forged security information can trick a NFC device into accepting an emulated or cloned NFC device as the original. Just like other RFID tags, also NFC devices can be *deactivated* by physically destroying the NFC chip or any other critical part of the device (e.g. mechanically or using a microwave), and NFC tags can be *detached* from a tagged item and subsequently associated with a different item.
- With respect to communication, messages exchanged between NFC devices are vulnerable to ***eavesdropping*** as well, although the communication distance between two NFC devices is smaller than that of most other RFID technologies, reducing the risk of eavesdropping. Eavesdropping can lead to *privacy infringement* and *replay attacks*: repeating one side of the recorded communication to simulate that NFC device; and *man-in-the-middle (relay) attacks*: placing a rogue device in between the two communication NFC devices, such that that all communication goes unnoticed through this third device. Smartly modifying this communication could for example in payment systems lead to charging the wrong electronic wallet. Furthermore, communication may be *jammed* by using powerful transmitters or by shielding.
- Finally, an often overlooked aspect when discussing the security threats associated with RFID (that applies to NFC applications as well), is the interaction with back-end systems. ***Attacks to the back-end system*** can affect the entire NFC application, and are therefore a serious threat. Examples include rogue tags that contain viruses [7] or other RFID malware that spread in the back-end system, tags that contain data that make the systems crash, e.g. due to their unexpected length, causing buffer overflows, or simply tags (or devices programmed to appear as tags) that (over)load the system with incorrect information.

2.2 All NFC devices are readers/writers

All NFC devices support the active communication mode. Therefore, all NFC devices are potential NFC readers. For example, when NFC has become a standard feature of mobile phones, many people will actually carry an NFC reader with them all the time. As a consequence, you could be surrounded by a crowd of potential readers, that are capable of communicating with the NFC devices and tags you carry with you, without your knowledge. This new feature of NFC creates a number of threats.

- People's privacy will be threatened, as certain information on NFC devices and tags can be read by everybody. This includes the unique ID of an NFC chip, which can always be read, but also non-secured personal data stored on the device or tag.
- We expect to see mobile phones infected with malware that uses the NFC reader capability to scan and attack other NFC devices or tags in its vicinity. Possible attacks include unauthorised reading (confidential information like credit card data, and usernames and passwords) or unauthorised writing. The NFC interface also opens up a new channel to distribute viruses and other malware directed at the device containing the NFC itself.
- When carrying NFC readers has become the norm, the incentive to try to rewrite NFC tag data on e.g. products in shops to get a cheaper price will increase.

2.3 All NFC devices can emulate a tag

Similarly, if many NFC devices implement card emulation mode (and whether they will is unclear at the moment), many people will be carrying a device that can be programmed to look like any conceivable NFC tag all the time. Again there may be the incentive to write software that allows one to emulate tags of cheap products, or to emulate access tickets for the cinema or access card to office buildings and the like. The impact of this threat appears to be small due to the limited reading distance.

2.4 Near field communication not enforced

Many organisations try to assure their customers that NFC is secure, as the reading distance of NFC is 10 centimetres at maximum. In fact this is only true for NFC readers that have "normal" antennas, such as the ones current mobile NFC phones are equipped with. However, an NFC reader with a more powerful antenna is not restricted to this distance.
Moreover, reading distances of 25 cm [8] and 40-50 cm [9] have been reported for NFC systems [10]. This distance is mostly limited by the fact that the NFC tag needs to be powered by the electro magnetic field emanating from the reader. For battery powered NFC devices this is not an issue, so reading distances may actually be even larger. The consequence is that it is still possible to communicate from a greater distance with NFC devices and tags than organisations claim.

This induces two separate risks: first, the reading distance cannot be enforced by the tag alone and longer range eavesdropping is possible. But there is a separate risk of unwarranted perceived security. Organisations and individuals may feel that it is not necessary to secure data on NFC devices or tags that they carry with them, because they assume their data is secure from everything that is further away than 10 cm. Because this is not true, this perceived security threatens the actual security of everything that is accessible through an NFC interface.

2.5 NFC as gateway to attached device

NFC as communication mechanism on more complex devices such as mobile phones or PDAs opens up a new entrance to these devices. The same happened with the introduction of Bluetooth on mobile devices, but an important difference is that NFC does not have Bluetooth's undiscoverable mode. On top of that, the GSMA has standardised the NFC-SIM link (called SWP, for Single-Wire Protocol) that enables access through NFC to confidential data on the SIM even if the device is turned off or contains no batteries.
Therefore NFC creates (1) an always open input channel to an NFC-enabled device, making the device extra vulnerable for unauthorised reading and hacking attacks; and (2) an always open output channel, out of which applications may leak information to any passing writable NFC device or tag.

2.6 Interference among multiple NFC applications on single device

Another impact of using one NFC interface on devices that contain multiple NFC applications is the risk of improper application separation. In such a system, all applications use the same interface to communicate with the outside world. This introduces the risk that one application is capable of interfering with or eavesdropping on the communication of another application that runs on the same device. Separation of applications (e.g. when running in a sandbox) is undermined in such a case. Remember that many current NFC applications are high value applications, such as credit cards and public transport ticketing. The threat of malware that is capable of gaining access to such high value applications is not one that should be underestimated.

2.7 No security standard

As explained in the introduction, NFC is not equivalent to Mifare. NFC specifications do not provide a security standard or functions for authentication and access control, as for example for Bluetooth or WiFi, leaving it up to the application developer to properly secure data and communication on NFC devices or tags. Due to time constraints or lack of experience, the security of NFC applications may be badly implemented or even non-existent, leaving the end-user vulnerable to all kinds of threats.

2.8 Unintended pairing between NFC devices

Because NFC devices are intended to operate autonomously, they may connect to each other without explicit user interaction. This is cumbersome when multiple devices are in range: in that case, the device one connects to is not obvious. For example, in crowds (like the subway, on festivals) NFC mobile phones may connect to each other or to NFC (credit) cards in someone's wallet. This problem is similar to unintended Bluetooth pairing, but with a smaller likelihood to the limited reading distance.

2.9 Privacy

Last, but not least, privacy issues are raised by the use of NFC as well. In fact, the previous paragraphs have already touched upon some of these. To summarise those for completeness, privacy is threatened by:
- the possibility of unauthorised reading of tags,
- the fact that all NFC devices are potential readers,

- the fact that near field communication is not enforced, and that
- NFC can act as a gateway to the attached device

Furthermore, applications using NFC may impose further privacy infringements. They may collect and show a lot of data about their users without those users being aware of this. This is due to the fact that interaction between devices does not necessarily require explicit user interaction, and may not enforce a secure from of access control. For instance, in public transport, all details of a traveller's journeys can be stored. In payment applications, the fact that the user also carries a loyalty card may automatically be detected, even if the user would prefer not to show this loyalty card this time. The facts that users are not aware of which personal information is collected from their NFC and stored, and that users may be powerless to prevent this from happening, threatens their privacy.

3 Possible countermeasures

This chapter covers possible countermeasures for the NFC security threats discussed in the previous chapter. We again summarise the RFID countermeasures applicable to NFC as well (see [4,5,6]), before discussing NFC specific countermeasures.

3.1 RFID countermeasures applicable to NFC

Below we summarise the countermeasures that apply to both RFID and NFC.

- To avoid unauthorised access to NFC tags one can use tags that are capable of authenticating a reader, so that only authorised readers can read the tag's contents. Of course authentication should include more than simply checking the reader's ID, to prevent readers with falsified IDs from gaining access. NFC devices can be shielded by placing it in a Faraday Cage when not in use.
- In order to secure NFC devices from unauthorised modifications, apart from the mechanisms discussed in the previous item, the use of read-only tags is the most obvious solution. Another option, which also secures against unauthorised reads, is to use only the tag's read-only unique ID, and store all relevant data in a back-end system. The downside to this solution is the required connection of a tag reader with this back-end system.
- Authenticity of the data on the tag can be assured by signing the data the moment the tag is issued. This so called passive authentication also (partly) prevents unauthorised modifications; copying data form a valid tag on another tag may still be possible however.
- Privacy can be enhanced by changing the normally static tag's unique ID to a random number that changes each time the tag is activated. This prevents the possibility of following a tag's (and thus the tag's carrier's) whereabouts.
- The main countermeasure against attacks on the NFC communication link is proper encryption of the communication. This helps protecting against eavesdropping, and thus also against privacy infringement. If the integrity, authenticity, and freshness of the communication are guaranteed as well, replay attacks and man-in-the-middle attacks are also prevented. If encryption is not sufficient or not possible due to NFC tag functionality or timing restrictions, the effects of eavesdropping can be reduced by communicating as little as possible over the air, e.g. by only using the tag ID. Jamming transmitters can be detected using permanently installed field detectors or by performing random measurements, and be subsequently removed.
- A close mechanical connection between the NFC tag and the tagged item is a countermeasure against physical destruction and detachment of the tag, as it makes it difficult to destroy the tag or remove it without damaging the tagged item.
- To avoid attacks at the back-end, next to regular security measures for gateways and servers, NFC readers should authenticate tags and check their content. Moreover, NFC readers should be prepared to gracefully and securely handle tags that do not conform to the expected and specified behaviour. For example, readers should not assume that data obeys the expected format, and should truncate data that exceeds the expected length.

3.2 Using the UI of the NFC device

Unlike RFID tags, NFC devices may have some user interface (UI) that can be used to query the user and to ask for user input. This is a tremendous advantage. For instance, unauthorised access to the NFC tag can be prevented by requiring an additional action by the user, e.g. pressing OK or inserting a PIN code, to activate the NFC device. Visual feedback to the user about the context of a transaction can help preventing man-in-the-middle attacks. For example, presenting the final amount to be paid to the user on the display of his/her device before accepting the payment will prevent changes to this amount by malicious parties (provided the final amount is encoded in the accept message sent from the device). In any case, it is required that there is a trusted path between the NFC tag and the UI of the device. If not, malicious software on the device itself can alter information presented to the user or entered by the user, thus bypassing the security measure altogether.

3.3 Using the processing power and memory capabilities of the NFC device

The device connected to the NFC interface may have considerably more resources (memory and CPU) than a typical RFID tag. Hence, the NFC device may be able to use strong(er) cryptography, and be able to encrypt and sign messages and decrypt, authenticate, and/or verify the integrity of incoming messages. In particular, active authentication (where the tag and the reader engage in a challenge-response protocol) prevents cloning of tags, offering stronger protection than passive authentication (where the data on the tag is signed once when the tag is issued). Moreover, (privacy) sensitive data can be stored on the device instead of in the backend systems. This enables more privacy friendly application designs, and may require less stringent security controls in the backend systems as they store less sensitive data.

3.4 Using the Secure Element of the NFC device

With respect to NFC devices such as mobile phones, “secure NFC” is referred to as the addition of a smart card to a mobile phone, which is used by NFC applications to securely store sensitive data. This smart card, the so-called “Secure Element” (SE), can be one of the following:

- *Secure storage area on the SIM card*: ETSI is currently in the process of specifying and standardising a new type of SIM card, which is capable of running applications and which also contains secure storage areas.
- *Embedded in the mobile phone*: slowly more mobile phones are coming on the market with embedded smart cards, which are reachable through the phone’s NFC interface.
- *A removable smart card*: removable smart cards on e.g. microSD or MMC that contain a microprocessor and data storage area can be used as SE as well.

Possibly we will see NFC mobile phones containing a combination of different SEs in the nearby future.

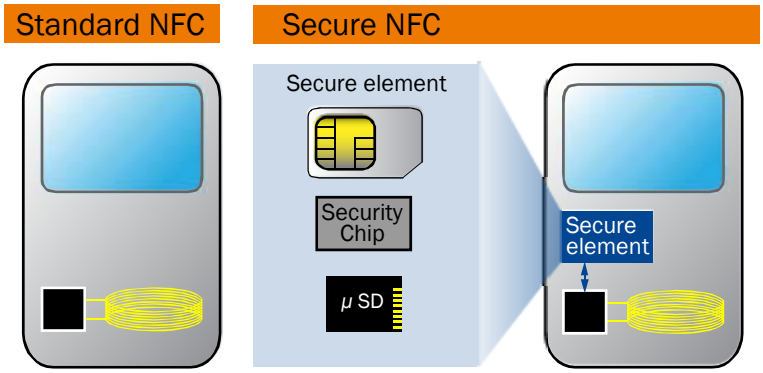

Figure 2: The three Secure Element possibilities

The inclusion of a SE to NFC mobile phones is to protect confidential data and applications from unauthorised access, either by mobile malware, an NFC reader, or even the user. This is achieved by regulating read and write access to the SE using keys, so that only signed applications of trusted sources can be installed on the SE, and data on the SE can be read only when presenting the right access key. The organisation handling this process effectively controls access to the SE, and should therefore be reliable.

Current SEs are designed in such a way that access through NFC to the SE is possible even when the phone's battery is removed. Although this offers the advantage of continuous availability, the user is never able to turn access to the SE off. Therefore current SEs come with activation levels that the user can choose: always accessible (even if the phone is off), not accessible when phone is off, ask for confirmation first, or ask for SE pass code first.

There are some concerns with this approach however. The current design of the SE does not allow the end-user to store personal data on the SE to his liking. Furthermore, there are a number of important yet unresolved issues with respect to the SE, such as the separation of security domains and how external applications are directed to the right data area, emulating multiple NFC cards on one phone, handling multiple SEs, etc. Before the Secure Element truly enables Secure NFC, its design and usage will have to mature.

3.5 Educating end-users

Last, but certainly not least, educating end users is a very important countermeasure. Users need to be educated about the risks of having "always on" connections, As with Bluetooth, NFC users' contact lists, calendars and other potentially sensitive company data may be exposed to wireless snoops if they are careless about managing their wireless status. It is important that users know at all times the status of their devices, such as whether they are configured to automatically connect with nearby NFC devices. If the users fail to understand the risks and fail to manage the security of the devices they own, no technical countermeasures will help prevent security breaches.

Educating users helps, but proper and consistent device and user interface design are equally important to ensure that the devices are easy to operate, easy to understand, and that the security measures do not interfere too much with the daily use of the device.

4 TNO's role

TNO Information and Communication Technology is a unique centre of innovation in the Netherlands that brings together the ICT and Telecom disciplines of TNO. We help companies, government bodies and (semi-)public organisations to realise successful innovations in ICT. Value creation for clients is our priority, and our added value lies in the combination of innovative strength and in-depth knowledge. Our approach to innovation is integrated and practical. Our research involves more than the technologies themselves. Where necessary, we also focus on user-friendliness, financial aspects, and business processes. We support the implementation process by carrying out technical and market trials. We are also specialists in innovation strategy and policy, and our extensive ICT expertise is a valuable resource that can be used to address issues in the wider community.

We believe NFC is a potentially high impact technology, both in terms of the possible new applications it brings and regarding the societal issues that may arise from its use. TNO, due to its independent nature, is in the perfect position to address both these issues and strike the right balance.

5 Conclusions & Recommendations

NFC is often positioned as a technology that enables “one-touch” applications (comparable to the “one-click” applications on the Internet). The primary example is the “touch-and-go” payment for goods using for example an NFC enabled mobile phone that behaves as a wallet or a payment card. Such applications are certainly possible, but implementing them may not be as easy as sometimes suggested. Applications like this have strong security requirements, while NFC is vulnerable to a certain number of attacks that are not addressed by the NFC standards themselves. As an RFID technology, NFC inherits risks associated with RFID. Moreover, there are a number of new threats that one has to be aware of when deploying NFC technology.

The reading distance of NFC is not enforced, giving users a false sense of security. Instead of the intended 10 cm, NFC tags can actually be accessed from 25-50cm away. Secondly, NFC devices can be used as NFC readers, or can be programmed to emulate other tags. In the first case, for example when NFC becomes standard on mobile phones, many people in a group will actually be carrying a potential NFC reader. NFC readers are then effectively all around us, imposing a possible privacy threat. In the second case, fake tags that interfere with existing systems are readily available. Thirdly, NFC is a new gateway, or attack point, to and from the device it is attached to. Sometimes this is true even if the device itself is switched off, as is the case with certain types NFC devices where the security element (SE) attached to the NFC tag can be powered completely by an external NFC device. Finally, the widespread use of NFC technology may, if not properly used, lead to even more privacy infringements

Fortunately, there are a number of countermeasures that exceed the possibilities one typically has with RFID only systems. NFC devices typically have a user interface that can be used to warn, signal, or ask the user. Moreover, NFC devices have more resources (in terms of CPU power and memory size) that can be used to implement stronger security. Finally, the use of NFC in mobile phones allows one to use the Secure Element to enhance the security of the application.

The NFC security landscape is diverse: new threats, and new countermeasures to mitigate them. The real security of NFC based systems will become apparent once the technology is used in the wild.

6 Glossary

CPU	Central Processing Unit
ECMA	European Computer Manufacturers Association
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
GSMA	GSM Association
ID	Identifier
ISO	International Organization for Standardization
MMC	Multi-Media Card
NFC	Near Field Communication
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RF	Radio Frequency
RFID	Radio Frequency Identification
SD	Secure Digital
SE	Secure Element
SIM	Subscriber Identity Module
SWP	Single Wire Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunications System
WiFi	Wireless Fidelity

7 Bibliography

[1] Klaus Finkenzeller. RFID Handbook. Wiley, Chicester, 2004

[2] ISO/IEC 18092, “Information Technology- Telecommunications and information exchange between systems- Near Field Communication - Interface and Protocol (NFCIP-1)”.

[3] ECMA, “Near Field Communication White Paper”, TC32-TG19/2004/1

[4] Thijs Veugen, Marjo Geers, Johanneke Siljee: Een security analyse van RFID systemen, Informatiebeveiliging, nummer 6, Oktober 2006 (Dutch only, for an English version, see Marc van Lieshout et al, RFID Technologies: Emerging Issues, Challenges and Policy Options, EUR 22770 EN, May 2007)

[5] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID systems and security and privacy implications. In 4th Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2523, pages 454-469, Redwood Shores, CA, USA, August 13-15 2002. Springer.

[6] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In 1st Int. Conf. on Security in Pervasive Computing, LNCS 2802, pages 201-212, Boppard, Germany, March 12-14 2003. Springer.

[7] Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?," percom, pp. 169-179, Fourth IEEE International Conference on Pervasive Computing and Communications (PerCom'06), 2006

[8] Ilan Kirschenbaum1 Avishai Wool, “How to Build a Low-Cost, Extended-Range RFID Skimmer” 15th USENIX Security Symposium, pp. 43–57, 2006.

[9] Ziv Kfir, Avishai Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard," pp. 47-58, First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), 2005

[10] Gerhard P. Hancke, "Practical Attacks on Proximity Identification Systems (Short Paper)," pp. 328-333, 2006 IEEE Symposium on Security and Privacy (S&P'06), 2006